



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 10/800,806 | 03/15/2004 | Jeffrey A. Von Arx | 020.0328.US.UTL | 1609 |

49475 7590 12/06/2007
CASCADIA INTELLECTUAL PROPERTY
500 UNION STREET
STE.1005
SEATTLE, WA 98101

| |
|----------|
| EXAMINER |
|----------|

YOUNG, NICOLE M

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2139

| | |
|-----------|---------------|
| MAIL DATE | DELIVERY MODE |
|-----------|---------------|

12/06/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

| | | | |
|------------------------------|-------------------------------|--------------------------------|--|
| Office Action Summary | Application No. 10/800,806 | Applicant(s) VON ARX ET AL. | |
| | Examiner Nicole M. Young | Art Unit 2139 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 3/15/2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-81 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-81 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 15 March 2007 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date <u>See Continuation Sheet</u> . | 6) <input type="checkbox"/> Other: _____ |

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :7/06/2004, 8/25/2005, 9/19/2005. 11/21/2005, 02/08/2006.

DETAILED ACTION

This communication replaces the Office Action sent September 19, 2007 and includes rejections for claims 69-77.

This communication is in response to the application filed March 15, 2004. Claims 1-81 are pending. The Applicant has used the language "means for" within the claims. The Examiner considers 112 6th paragraph to be invoked.

Specification

The disclosure is objected to because of the following informalities:

Page 4 line 9, delete the extra comma after PHI,

Page 11 line 18, insert serial number of commonly assigned application,

Page 12 line 2, insert serial number of commonly assigned application.

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: the terms "encrypter", "repeater", and "programmer" in claims 3, 6, and 7 respectively, and throughout the rest of the claim language.

Appropriate correction is required.

Claim Objections

Claims 3, 32 objected to because of the following informalities:

In claims 3 and 32 remove the extra space after "and ;",

Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 59, 78, and 81 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 59 recites "defining means", "establishing means", and authentication means". As 112 6th paragraph is considered to be invoked, each of these "means for" statements must have a specific physical structure in the specification. The Examiner cannot determine this from the specification.

Claim 78 recites "providing means", "commencing means", and transacting means". As 112 6th paragraph is considered to be invoked, each of these "means for" statements must have a specific physical structure in the specification. The Examiner cannot determine this from the specification.

Claim 81 recites "providing means", "requesting means", "receiving means", "commencing means", and "transacting means". As 112 6th paragraph is considered to be invoked, each of these "means for" statements must have a specific physical structure in the specification. The Examiner cannot determine this from the specification.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-29, 60-68, 79 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1, 60 and 79 are systems. There is not enough hardware structure within the claim language to support a system. The limitations are interpreted to be accomplished through the use of software, which is non-statutory subject matter under 35 U.S.C. 101.

Claims 2-29 and 61-68 are dependent on claims 1 and 60 respectively and do not provide further hardware.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3, 5-10, 17-20, 27-29 and 59 are rejected under 35 U.S.C. 102(e) as being anticipated by **Thompson (7,027,872)**, herein referred to as Thompson.

Claim 1 discloses a system for securely authenticating a data exchange session with an implantable medical device, comprising:

a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session (Thompson column 8 lines 18-50, key for encrypting data from a particular IMD); and

an external source to establish a secure connection with a secure key repository to securely maintain the crypto key (Thompson, column 10 lines 39-42, key source provides encryption keys), and to authenticate authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository (Column 10 lines 21-26, encrypted sensitive information).

Claim 2 discloses a system according to Claim 1, wherein the external source transacts a data exchange session using the crypto key to authenticate the data (Thompson, column 10 lines 28-43, data is encrypted before exchanged).

Claim 3 discloses a system according to Claim 2, further comprising:

an authentication component to employ the crypto key during the data exchange session, comprising at least one of:

a command authenticator to authenticate commands exchanged through the external source with the implantable medical device and (Thompson, column 4 lines 23-48 wherein "medical device program commands" are encrypted and sent to the IMD) ;

a data integrity checker to check the integrity of the data received by and transmitted from the external source (Thompson, column 4 lines 49-66, message integrity checks); and

a data encrypter to encrypt the data received by and transmitted from the external source (Thompson, Figure 4 both the Programmer and the Clinician computer have encryption engines and decryption engines).

Claim 5 discloses a system according to Claim 1, further comprising:

a key generator to statically generate the crypto key, and to persistently store the crypto key in the secure key repository (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys).

Claim 6 discloses a system according to Claim 5, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, a secure database, a physical token, and a repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

Claim 7 discloses a system according to Claim 5, wherein the crypto key is securely retrieved from the secure key repository through a programmer (Thompson, Figure 4

Art Unit: 2139

key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

Claim 8 discloses a system according to Claim 1, further comprising:

a key generator to dynamically generate the crypto key (Thompson, Figure 4 key source 228, and column 8 lines 48-66 and column 910-49; the key source distributes many different kind of algorithms including the generation of session keys).

Claim 9 discloses a system according to Claim 8, wherein the crypto key is stored on at least one of the implantable medical device, a patient designator, and a repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

Claim 10 discloses a system according to Claim 8, wherein the crypto key is securely retrieved from the secure key repository through at least one of a programmer and a repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

Claim 17 discloses a system according to Claim 1, further comprising:

a secure database to maintain the crypto key (Thompson column 8 lines 18-47 teaches a secure database); and

a secure server providing the crypto key through a secure connection (Thompson column 9 lines 10-49 teaches a tunneled connection).

Claim 18 discloses a system according to Claim 17, wherein the secure connection comprises at least one of a serial or hardwired connection and a secure network connection (Thompson column 9 lines 63-67 and column 10 lines 1-10 teach hardwired secure connection).

Claim 19 discloses a system according to Claim 17, wherein the external source comprises a programmer repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

Claim 20 discloses a system according to Claim 19, wherein the crypto key is provided from the programmer to a repeater repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

Art Unit: 2139

Claim 27 discloses a system according to Claim 1, wherein the crypto key comprises at least one of a 128-bit crypto key and a symmetric crypto key (Thompson column 9 lines 50-64 teaches “a 128 bit hashed representation of a message” and a public key).

Claim 28 discloses a system according to Claim 1, wherein the crypto key comprises at least one of a statically generated and persistently stored crypto key, dynamically generated and persistently stored crypto key, a dynamically generated and non-persistently stored session crypto key (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer, both would have a secure database and designate patients).

Claim 29 discloses a system according to claim 1, wherein implantable medical device comprises at least one of an implantable cardiac device, neural stimulation device, and drug therapy dispensing device (Thompson column 2 lines 39-64 teach implantable cardiac devices).

Claims 59 and 30 disclose an apparatus and method for securely authenticating a data exchange session with an implantable medical device, comprising:

means for defining a crypto key uniquely associated with an implantable medical device to authenticate data during a data exchange session (Thompson column 8 lines 18-50, key for encrypting data from a particular IMD);

means for establishing a secure connection from an external source with a secure key repository securely maintaining the crypto key (Thompson, column 10 lines 39-42, key source provides encryption keys, column 10 lines 21-26, encrypted sensitive information); and

means for authenticating authorization to access data on the implantable medical device by means for securely retrieving the crypto key from the secure key repository (Thompson column 8 lines 48-67 teach authentication).

Claim 60 is rejected under 35 U.S.C. 102(e) as being anticipated by **Lee (US 6, 442, 432)** herein referred to as Lee.

Claim 60 discloses a system for securely transacting a data exchange session with an implantable medical device, comprising:

a short range interface to provide communication with an implantable medical device by authenticating access to a securely maintained crypto key (Lee column 11 lines 2-24 and column 15 lines 38-60);

a long range interface to commence a data exchange session upon successful access authentication with the implantable medical device, and to transact the data exchange session using the crypto key (Lee column 16 lines 33-49).

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 4, 61, and 78-81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson (7,027,872), herein referred to as Thompson and further in view of Lee (US 6, 442, 432) herein referred to as Lee. 69

Thompson teaches the limitations of claim one as rejected above. Thompson does not teach but Lee teaches **claim 4**, which discloses a system according to Claim 1, further comprising:

a short range interface logically defining a secured area around the implantable medical device in which to establish the secure connection (Lee column 11 lines 3-24 and column 15 lines 38-60); and

a long range interface logically defining a non-secured area extending beyond the secured area in which to transact the data exchange session (Lee column 16 lines 33-49).

It would be obvious to a person of ordinary skill in the art at the time of invention to use Lee's secure communication sessions with Thompson's secure connections and encryption methods. Lee's method of storing encrypted data on the implantable

Art Unit: 2139

medical device offers the advantage of protecting sensitive data from access by unauthorized persons and protecting the medical device from improper snooping and improper instructions (Lee column 15 lines 63-67 and column 16 lines 1-4).

Claims 61 and 70 disclose a system according to Claim 60, wherein the patient health information is maintained in an encrypted form (Thompson, column 10 lines 28-43, data is encrypted before exchanged).

Claims 68 and 79 disclose a system according to Claims 60 and 69, wherein the long range interface is augmented using one or more repeaters (Thompson figure 1 programmer (extender) 112 and associated text).

Claims 69 and 78 disclose an apparatus for securely transacting a data exchange session with an implantable medical device, comprising:

means for providing communication with an implantable medical device by means for authenticating access to a securely maintained crypto key using a short range interface (Lee column 11 lines 3-24 and column 15 lines 38-60);

means for commencing a data exchange session by means for transitioning to long range interface upon successful access authentication with the implantable medical device (Lee column 16 lines 33-49).; and

means for transacting the data exchange session by accessing patient health information stored on the implantable medical device using the crypto key Thompson, column 10 lines 28-43, data is encrypted before exchanged).

It would be obvious to a person of ordinary skill in the art at the time of invention to use Lee's secure communication sessions with Thompson's secure connections and encryption methods. Lee's method of storing encrypted data on the implantable medical device offers the advantage of protecting sensitive data from access by unauthorized persons and protecting the medical device from improper snooping and improper instructions (Lee column 15 lines 63-67 and column 16 lines 1-4).

Claim 79 discloses a system for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

a secure server to provide identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key (Lee Figure 1 and associated text teaches the use of a server and column 16 lines 3-33 teaches authentication);

a secure external source to request the crypto key via a secure connection based on the identification of and authentication to access the implantable medical device, and to receive the crypto key (Thompson, column 10 lines 39-42, key source provides encryption keys and Lee column 16 lines 3-33 teaches authentication); and

a long range interface to commence a data exchange session upon successful access authentication with the implantable medical device, and to transact the data exchange session using the crypto key (Lee column 16 lines 33-49).

It would be obvious to a person of ordinary skill in the art at the time of invention to use Lee's secure communication sessions with Thompson's secure connections and encryption methods. Lee's method of storing encrypted data on the implantable medical device offers the advantage of protecting sensitive data from access by unauthorized persons and protecting the medical device from improper snooping and improper instructions (Lee column 15 lines 63-67 and column 16 lines 1-4).

Claims 80 and 81 disclose a method for securely transacting a data exchange session with an implantable medical device through secure lookup, comprising:

providing identification of and authentication to access an implantable medical device by authenticating access to a securely maintained crypto key (Thompson, column 10 lines 28-43, data is encrypted before exchanged and Lee column 16 lines 3-33 teaches authentication);

requesting the crypto key via a secure connection based on the identification of and authentication to access the implantable medical device (Thompson, column 10 lines 39-42, key source provides encryption keys and Lee column 16 lines 3-33 teaches authentication), and

receiving the crypto key (Lee column 16 lines 33-49);

commencing a data exchange session by transitioning to long range interface upon successful access authentication with the implantable medical device(Lee column 16 lines 33-49); and

transacting the data exchange session using the crypto key (Lee column 16 lines 33-49).

It would be obvious to a person of ordinary skill in the art at the time of invention to use Lee's secure communication sessions with Thompson's secure connections and encryption methods. Lee's method of storing encrypted data on the implantable medical device offers the advantage of protecting sensitive data from access by unauthorized persons and protecting the medical device from improper snooping and improper instructions (Lee column 15 lines 63-67 and column 16 lines 1-4).

Claims 11-16, 62, 63, and 65-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Thompson (US 7,027,872)** and **Lee (6,442,432)**, and further in view of **Eckmiller et al. (US 6,493,587)** herein referred to as Eckmiller.

Thompson teaches the limitations of claim 1 rejected above. Thompson and Lee do not teach but Eckmiller teaches **claims 11 and 12**, which disclose a system according to Claim 1, wherein the crypto key is maintained on the implantable medical device, further comprising:

a short range telemetry interface retrieving the crypto key through short range telemetry (Eckmiller column 9 lines 28-53, passes public key).

It would have been obvious to a person of ordinary skill in the art at the time of the invention to utilize Eckmillers method of storing and retrieving keys because it offers the advantage of preventing the unauthorized access to important functions of neuroprostheses and unauthorized imitation of components (Eckmiller column 3 lines 5-15).

Claim 13 discloses a system according to Claim 11, wherein the external source comprises a programmer (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer).

Claim 14 discloses a system according to Claim 13, wherein the crypto key is provided from the programmer to a repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer; and Thompson figure 1 programmer (extender) 112 is interpreted to be the repeater.

Claim 15 discloses a system according to Claim 11, wherein the external source comprises a patient designator (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer wherein the clinician computer is interpreted to be the patient designator).

Claim 16 discloses a system according to Claim 15, wherein the crypto key is provided from the patient designator to at least one of a programmer and a repeater (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer; within the asymmetric key algorithm the public key would be passed from the clinician computer to the programmer).

Claims 62 and 71 discloses a system according to Claim 60 and 69, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

- a short range telemetric connection with the implantable medical device;
- a short range telemetric device to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device (Eckmiller column 9 lines 28-53, passes public key).

Claims 63 and 72 discloses a system according to Claim 60 and 69, wherein the authenticating with the implantable medical device is through a patient designator, further comprising:

- a short range telemetric connection with the implantable medical device (Eckmiller column 9 lines 28-53, passes public key);

a patient designator to request the crypto key from the implantable medical device, and to receive the crypto key from the implantable medical device (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer wherein the clinician computer is interpreted to be the patient designator).

Claims 65 and 74 disclose a system according to Claims 60 and 69, wherein the patient health information is maintained in the implantable medical device in unencrypted form and is accessible in the unencrypted form exclusively through a short range telemetric connection (Eckmiller column 9 lines 28-53, passes public key).

Claims 66 and 75 disclose a system according to Claim 65 and 74, wherein the authenticating with the implantable medical device is through short range telemetry, further comprising:

a short range telemetric connection with the implantable medical device (Eckmiller column 9 lines 28-53, passes public key);

an external source to send a session crypto key to the implantable medical device (Thompson, Figure 4 key source 228, and column 8 lines 48-66, the key source distributes symmetric keys and asymmetric keys to the programmer and clinician computer wherein the clinician computer is interpreted to be the patient designator); and

an encrypter to encrypt the patient health information maintained in the implantable medical device (Thompson, Figure 4 both the Programmer and the Clinician computer have encryption engines and decryption engines).

Claims 67 and 76 disclose a system according to Claims 60 and 69, wherein the authenticating with the implantable medical device is through a patient designator, further comprising:

a patient designator to establish a short range telemetric connection with the implantable medical device, and to send a session crypto key to the implantable medical device(Eckmiller column 9 lines 28-53, passes public key); and

an encrypter to encrypt the patient health information maintained in the implantable medical device (Thompson, Figure 4 both the Programmer and the Clinician computer have encryption engines and decryption engines).

Claims 21-26, 64, and 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thompson (US 7,027,872), and further in view of Wheeler et al. (2002/0016913) herein referred to as Wheeler.

Thompson teaches the limitations of claims 1 and 60 as rejected above. Thompson does not teach but Wheeler teaches **claims 21, 64, and 73**, which discloses a system according to Claim 1, 60, and 69 further comprising:

a physical token to maintain the crypto key; and

a reader to retrieve the crypto key by accessing the physical token in paragraphs [0066] and [0279]. It would be obvious to one of ordinary skill in the art at the time of invention to combine Thompson's security method with Wheeler's use of a smart card. As it states in Lee paragraph [0444] "it will now be understood and appreciated that a device constructed in accordance with the present invention preferably has the following aspects: high integrity, tempested, immune to all known chip card attack".

Claim 22 discloses a system according to Claim 21, further comprising:

a physical label to specify the crypto key on the physical token (Lee paragraphs [0066] and [0279] teach that a token can be a credit card).

Claim 23 discloses a system according to Claim 22, wherein the physical label comprises at least one of alphanumeric text, bar coding, and an outwardly-appearing indication (Lee paragraphs [0066] and [0279] teach that a token can be a credit card).

Claim 24 discloses a system according to Claim 21, further comprising:

internal storage to specify the crypto key on the physical token (Lee paragraphs [0066] and [0279]).

Claim 25 discloses a system according to Claim 24, wherein the internal storage comprises at least one of a transistor, a memory circuit, an electronically readable storage medium, and a magnetically readable storage medium (Lee paragraph [0279]).

Claim 26 discloses a system according to Claim 21, wherein the physical token is accessed using magnetic, optical, serial, and physical reading (Lee paragraph [0279]).

Claims 31-58 are the method of claims 2-29, and are rejected on the same basis as 2-29 above.

Note: Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion


The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nicole M. Young whose telephone number is 571-270-1382. The examiner can normally be reached on Monday through Friday, alt Fri off, 8:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

NMY
9/10/2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100